STATE OF ALABAMA

Information Technology Policy

Policy 670-06: Log Management

Log management is essential to ensuring that computer security records are stored in sufficient detail for an appropriate period of time. Log management activities include log generation, transmission, storage, analysis, and disposal; while protecting the confidentiality, integrity, and availability of logs.

OBJECTIVE:
Establish log management responsibilities for the State of Alabama computing environment.

SCOPE:
This policy applies all State of Alabama employees, contractors, vendors, and business partners responsible for the administration, development, or security management of any information system resources that store or process State data and support event logging.

RESPONSIBILITIES:
IT Managers shall prioritize log management appropriately throughout their respective organization, create and maintain a secure log management infrastructure, establish procedures for log management (including incident response), and provide proper training for all staff with log management responsibilities.

Security Administrators and Information Security Officers shall manage and monitor the log management infrastructure, configure logging on security devices (e.g., firewalls, network-based intrusion detection systems, antivirus servers), and assist others with configuring logging and performing log analysis.

System and Network Administrators shall configure logging on individual systems and network devices, perform regular maintenance of the logs and logging software, and proactively analyze log data to identify on-going activity and signs of impending problems.

Application Developers shall design or customize applications so they perform logging in accordance with logging requirements and applicable State standards.

ENFORCEMENT:
Refer to Information Technology Policy 600-00: Information Security.
http://isd.alabama.gov/policy/Policy_600-00_Information_Security.pdf

ADDITIONAL INFORMATION:
DEFINITIONS: Refer to Information Technology Dictionary
http://isd.alabama.gov/policy/IT_Dictionary.pdf

Signed by Jim Burns, Chief Information Officer

DOCUMENT HISTORY:

Version	Release Date	Comments
Original	12/12/2006	